

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

EDGE CAPTURE L.L.C., and EDGE  
SPECIALISTS, L.L.C.,

Plaintiffs,

v.

BARCLAYS BANK PLC, BARCLAYS  
CAPITAL INC., UBS AG, UBS  
FINANCIAL SERVICES INC., UBS  
SECURITIES LLC, WOLVERINE  
TRADING, L.L.C., AND WOLVERINE  
EXECUTION SERVICES, L.L.C.,

Defendants.

Civil Action No. 09 CV 1521

**JURY TRIAL DEMANDED**

Judge Charles R. Norgle, Sr.

Magistrate Judge Denlow

**AGREED PROTECTIVE ORDER**

The Court enters the following Protective Order pursuant to Federal Rule of Civil Procedure 26(c)(1).

1. The Court finds that the parties to this case may request or produce information involving trade secrets or confidential research and development or commercial information, the disclosure of which is likely to cause harm to the party producing such information.

2. As used in this Protective Order, these terms have the following meanings:

- (a) "Attorneys" means outside counsel of record.
- (b) "Party" means a named party in this case. "Person" means an individual or entity. "Producer" means a Person who produces information via the discovery process in this case. "Recipient" means a Person who receives information via the discovery process in this case.
- (c) "Document" has the meaning prescribed in Fed. R. Civ. P. 26 and 34.
- (d) "Source Code" means human-readable program statements written by a programmer or developer in a high-level or assembly language that are not directly readable by a computer. Source Code includes computer instructions and

data definitions expressed in a form suitable for input to an assembler, compiler, other translator, or other data processing module.

- (e) "Confidential" information is information concerning a Person's business operations, processes, or technical and development information within the scope of Rule 26(c)(1)(G), the disclosure of which is likely to harm that Person's competitive position, or the disclosure of which without a Confidential designation would contravene an obligation of confidentiality to a third party or to a court.
- (f) "Highly Confidential" information is information within the scope of Rule 26(c)(1)(G) that is current or future business or technical trade secrets and plans more sensitive or strategic than Confidential information, the disclosure of which is likely to significantly harm that Person's competitive position, or the disclosure of which without a Highly Confidential designation would contravene an obligation of confidentiality to a third party or to a court. As a general guideline, Documents designated as Highly Confidential shall be those Documents of a proprietary business or technical nature that would be of value to a competitor or potential customer of the Party or third party holding the proprietary rights thereto, and that should be protected from disclosure. Examples of such Documents include, but are not limited to, those disclosing a Party's trade secrets; technical or business information; technical practices; methods or other know-how; past, present or future marketing plans; past, present or future competitive analyses; product profit data or other projections; financial data; business strategy; and non-public agreements or relationships with third parties.
- (g) "Highly Confidential – Computer Source Code" information is the subset of Highly Confidential information comprising Source Code and designated pursuant to paragraph 8 below.
- (h) "Written Assurance" means an executed document in the form attached as Exhibit A.
- (i) "Edge" means Edge Capture L.L.C. and Edge Specialists, L.L.C., collectively.
- (j) "Barclays" means Barclays Bank PLC and Barclays Capital Inc., collectively.
- (k) "UBS" means UBS AG, UBS Financial Services Inc. and UBS Securities LLC, collectively.
- (l) "Wolverine" means Wolverine Trading, L.L.C. and Wolverine Execution Services, L.L.C., collectively.

3. A Party may designate as "Confidential," "Highly Confidential," or "Highly Confidential – Computer Source Code" those Documents, including interrogatory responses, other discovery responses, electronic media, or transcripts, that it in good faith contends to

constitute or contain Confidential, Highly Confidential, or Highly Confidential – Computer Source Code information. The following Documents or information shall not be designated “Confidential,” “Highly Confidential,” or “Highly Confidential – Computer Source Code”: (a) any information that at the time of disclosure to a Recipient is in the public domain; (b) any information that after disclosure to a Recipient becomes part of the public domain as a result of publication, excluding a violation of this Protective Order; (c) any information that a Recipient can show that it received, whether before or after the disclosure, from a source who obtained the information lawfully and under no obligation of confidentiality to the Producer; and (d) any information that a Recipient can show was independently developed by its personnel who did not have access to the producing Party’s Confidential, Highly Confidential, or Highly Confidential – Computer Source Code Documents.

4. All Confidential, Highly Confidential, or Highly Confidential – Computer Source Code Documents, along with the information contained in the Documents, shall be used solely for the purpose of this action and not for competitive purposes, and no Person receiving such Documents shall, directly or indirectly, transfer, disclose, or communicate in any way the contents of the Documents to any Person other than those specified in paragraphs 6 and 7. Prohibited purposes include, but are not limited to, use for competitive purposes or the prosecution of additional intellectual property rights.

5. A Person’s designation of information as Confidential, Highly Confidential, or Highly Confidential – Computer Source Code means that the Person believes in good faith, upon reasonable inquiry, that the information qualifies as such. A Person designates information in a Document or thing as Confidential, Highly Confidential, or Highly Confidential – Computer Source Code by clearly and prominently marking it on its face as “Confidential,” “Highly

Confidential – Attorneys’ Eyes Only,” or “Highly Confidential – Computer Source Code,” respectively. A Producer may make Documents or things containing Confidential, Highly Confidential, or Highly Confidential – Computer Source Code information available for inspection or copying without marking the original Documents or things as Confidential, Highly Confidential, or Highly Confidential – Computer Source Code, without forfeiting a claim of confidentiality, so long as the producer causes any copies of the documents or things to be marked as Confidential, Highly Confidential or Highly Confidential – Computer Source Code before providing them to the recipient or within a reasonable time after discovering an inadvertent failure to designate such copies. A Person designates information in deposition testimony as Confidential, Highly Confidential, or Highly Confidential – Computer Source Code by stating on the record at the deposition that the information is Confidential, Highly Confidential, or Highly Confidential – Computer Source Code or by advising all parties and the stenographer and videographer in writing, within fourteen (14) days after receipt of the deposition transcript, that the information is Confidential, Highly Confidential, or Highly Confidential – Computer Source Code. The deposition of any witness (or any portion of such deposition) that encompasses Confidential, Highly Confidential, or Highly Confidential – Computer Source Code information shall be taken only in the presence of Persons who are qualified to have access to such information. A person’s failure to designate a document, thing, or testimony as Confidential, Highly Confidential, or Highly Confidential – Computer Source Code does not constitute forfeiture of a claim of confidentiality as to any other document, thing, or testimony.

6. Absent written permission from the Producer or further order by the Court, the Recipient may not disclose Confidential information to any Person other than the following:

- (a) the Court, the jury, and personnel assisting the Court;
- (b) Attorneys and their office associates, legal assistants, and stenographic and clerical employees;
- (c) Persons who are believed in good faith to have authored or received it or employees of the Producer;
- (d) court reporters and videographers retained to transcribe and record testimony;
- (e) a Party's (i) inside counsel and their office associates, legal assistants, and stenographic and clerical employees, after execution of the attached Written Assurance and/or (ii) officers and employees directly involved in this case whose access to the information is reasonably required to supervise, manage, or participate in this case, after execution of the attached Written Assurance;
- (f) outside independent Persons who have been retained by a Party or its Attorneys to furnish technical or expert services, and/or to give expert testimony in this action, after execution of the attached Written Assurance and compliance with the requirements of paragraph 11 below;
- (g) outside independent Persons who have been retained by a Party or its Attorneys to provide assistance as mock jurors or focus group members, after execution of the attached Written Assurance, as well as a written verification by each such Person that they are not in the business of options trading; or
- (h) any other Person only upon order of the Court or upon written consent of the Producer.

7. Disclosure of Highly Confidential information shall be limited to the Persons designated in paragraphs 6(a), (b), (c), (d), (f), (g) and (h).

8. To the extent production of Source Code becomes necessary in this litigation, a Producer may elect to designate Source Code as "Highly Confidential – Computer Source Code." "Highly Confidential – Computer Source Code" information shall be subject to all of the restrictions and obligations applicable to Highly Confidential information and, unless the Producer and Recipient agree otherwise in writing, subject to the disclosure and review process described below.

- (a) Because of the highly sensitive nature of computer Source Code and because of the ease with which electronic media may be copied, transported, or stolen, computer Source Code designated as "Highly Confidential – Computer Source Code" may not be copied or stored by any person acting on behalf of a recipient permitted to have access to the same (an "authorized person"), except as expressly permitted herein.
- (i) No authorized person may create a copy of the Producer's Source Code or copy such computer Source Code onto any form of electronic media, including without limitation, hard drives, removable electronic media (such as diskettes, CD-ROM, DVD, PC card, flash media, etc.), or network servers, except that the computer Source Code may be loaded onto a computer's hard drive from electronic media (such as CD-ROM, DVD, PC card, flash media, etc.) on which it was produced, and/or into RAM or virtual RAM as required by the computer's operating system, for viewing, analysis, or other purposes.
- (ii) An authorized person may only load, view, analyze or otherwise use a Producer's Source Code on two designated computers ("the Review Computers"). Each Review Computer, at the time of such loading, viewing, analysis or other use, must be completely "stand alone" and not linked to any network, including a local area network ("LAN"), an intranet or the Internet. Neither Review Computer may be used to store or review the Source Code of any party other than the Producer. Each Review Computer must reside in a secure, locked room that only authorized persons can access located at a designated office of outside counsel for the Recipient or other mutually agreeable location ("the Review Location"). Only authorized persons shall access the Review Computer. At anytime a computer contains such computer Source Code, the Review Computer must remain stand alone and disconnected from any network (wired or wireless) until such time that all such computer Source Code have been erased from the computer's hard drive using a secure erase method. Notwithstanding this provision, if an authorized person uses an assembler, compiler, other translator, or other data processing module to test such computer Source Code, the computer on which the testing is performed may be connected to other computers necessary for testing, so long as the computers necessary for testing are not connected to any other computers, network, including a local area network, an intranet or the Internet whether by a wired, wireless or other connection type. The Recipient shall maintain a log of authorized persons who review the Source Code, including dates and times of review.
- (iii) Computer Source Code on removable electronic media must always be removed from the Review Computer, excluding the Review Computer's hard drive(s), when it is not currently being viewed, analyzed or otherwise used, and at such times of non-use, the Review Computer along with the

removable electronic media containing Source Code shall be securely stored to prevent theft or unauthorized access.

- (iv) If computer Source Code is loaded onto the Review Computer's hard drive, when the Review Computer is not currently being used for viewing and analysis or for other permitted purposes, it must be securely stored to prevent theft or unauthorized access.
  - (v) At the time an authorized person uses the Review Computer to view, analyze or otherwise use the Producer's computer Source Code, the Review Computer must remain within the control of that person.
- (b) The Producer's computer Source Code may not be transported in any way except to be delivered to the Review Location or returned to the Producer in a secure manner to be agreed upon by the Producer and Recipient, and for use at depositions, hearings, or trial. The Source Code must otherwise remain in the designated Review Location at all times, except for use at depositions, hearings, or trial. Additionally:
- (i) Source Code may be transported only at the direction of an authorized person to another authorized person.
  - (ii) The Producer's computer Source Code may not be transported or transmitted electronically over a network of any kind, including over a local area network (LAN), intranet or the Internet.
  - (iii) To the extent that a Recipient loads a Producer's computer Source Code onto a computer's hard drive, when the computer is no longer to be used for viewing and analysis of the computer Source Code or for other use involving the computer Source Code, the computer Source Code shall be erased from the hard drive by a secure erase method.
  - (iv) Unless the Producer otherwise agrees, any deposition involving the use of a Producer's Source Code (other than excerpts) shall be held at an office of outside counsel for the Producer or one of the two designated Review Location offices of outside counsel for the Recipient. For purposes of depositions, to the extent necessary, the Producer's Source Code may be shown to a deponent during a deposition on a Review Computer when conducted at one of the two designated Review Location offices of outside counsel for the Recipient. If the deposition is held at an office of outside counsel for the Producer, Producer and Recipient will reach an agreement to make Producer's Source Code available for use on a standalone computer in a form and manner agreeable to the Recipient for use during the deposition, and the computer shall be made available to the Recipient in advance of the deposition for inspection. If an agreement cannot be reached, the deposition shall, to the extent necessary, occur at one of the

two designated Review Location offices of outside counsel of the Recipient. For purposes of hearings or trial, to the extent necessary, the Producer and Recipient will reach a mutual agreement regarding the procedure for introducing Source Code (other than excerpts) at a hearing or trial or, if an agreement cannot be reached, approach the Court for resolution of any dispute.

- (c) An authorized person may excerpt portions of the Producer's computer Source Code onto paper or into an electronic document (such as into an electronically stored brief, report, or discovery response, or into an electronic document used to support or to create an electronic brief, report, or discovery response) for the purpose of creating submissions to or presentations for the Court, creating documents responding to discovery requests, creating presentations or materials to be used at settlement meetings, creating expert reports, or for use at a deposition, hearing, or trial, but only if the following provisions are satisfied.
  - (i) Any and all such computer Source Code excerpts shall be marked "Highly Confidential – Computer Source Code." To the extent such excerpts are submitted to the Court, presented at hearings, trial, or settlement meetings, disclosed in discovery responses, referenced in expert reports, or presented during a deposition, such excerpts shall be treated as information designated "Highly Confidential."
  - (ii) In the event that excerpts of the Producer's computer Source Code are copied electronically into a document for submission to the Court, presentation at a hearing, trial, or settlement meeting, responding to a discovery request, preparation of an expert report, or for use at a deposition, any such document or transcript shall be marked "Highly Confidential – Computer Source Code" and access thereto shall continue to be limited to authorized persons.
  - (iii) Excerpts of computer Source Code or electronic documents containing excerpts of computer Source Code may be created, edited, and/or stored on computers, computers or servers in or connected to networks, including over a local area network (LAN) or intranet, of law firms or of consulting organizations to which the authorized persons belong, provided that such excerpts or electronic documents containing excerpts are password protected so that only authorized persons may access the material.
  - (iv) Excerpts of computer Source Code or electronic documents containing excerpts of computer Source Code may be transported or transmitted electronically over a network, including over a local area network (LAN), intranet or the Internet, or downloaded from a server hosted by a law firm or a consulting organization to which the authorized person belongs, so long as all such excerpts or electronic documents containing excerpts are password protected so that only authorized persons may access the

material. Authorized persons may also view, access, or otherwise use excerpts of computer Source Code or electronic documents containing excerpts of computer Source Code over password-protected electronic conferencing systems such as NetMeeting.

- (v) All paper hard copies of excerpts of Source Code shall be securely destroyed in a timely manner if they are no longer in use (e.g., at the conclusion of a deposition).

9. Notwithstanding the provisions above, information designated "Highly Confidential" or "Highly Confidential – Computer Source Code" and information that contains copies, extracts, compilations, or summaries thereof, may not be disclosed, characterized, or otherwise communicated or made available in whole or in part to any patent prosecution attorney or patent agent, who is or may become responsible for prosecuting patent applications directed to automated derivatives trading. There are no restrictions, however, on outside counsel of record's ability to provide legal advice to a party on all issues that may impact this lawsuit, and/or the party's rights and remedies with respect to the patents-in-suit or related patents and patent applications, so long as there is no unauthorized disclosure of information designated "Confidential" "Highly Confidential" or "Highly Confidential – Computer Source Code."

10. Third parties producing Documents in the course of this action may also designate Documents as "Confidential," "Highly Confidential" or "Highly Confidential – Computer Source Code," subject to the same protections and constraints as the Parties to this action. A copy of this Protective Order shall be served along with any subpoena served in connection with this action. Each party requesting discovery from a third party (not a party to this action) by subpoena shall ensure that all parties in this action receive a copy of the subpoena.

11. Each Person appropriately designated pursuant to paragraph 6(f) to receive Confidential, Highly Confidential, or Highly Confidential – Computer Source Code information shall execute a "Written Assurance" in the form attached as Exhibit A. The party obtaining the

Written Assurance must serve it on all other parties within ten days after its execution. At least ten days before the first disclosure of Confidential, Highly Confidential or Highly Confidential – Computer Source Code information to an expert or consultant (or member of their staff), the party proposing to make the disclosure must serve the producer with a written identification of the expert or consultant and a copy of his or her curriculum vitae. If the producer has good cause to object to the disclosure (which does not include challenging the qualifications of the expert or consultant), it must serve the party proposing to make the disclosure with a written objection within ten days after service of the identification. Unless the parties resolve the dispute within ten days after service of the objection, the producer must move the Court promptly for a ruling, and the Confidential or Highly Confidential information may not be disclosed to the expert or consultant without the Court's approval.

12. Copies. A Party producing Documents as part of discovery must, upon request, furnish the requesting party with one copy of the Documents it requests, at the requesting party's expense. Before copying, the Parties must agree upon the rate at which the requesting party will be charged for copying.

13. The inadvertent or unintentional production of information without an appropriate designation of confidentiality shall not be deemed a waiver or impairment of any claimed protection of the confidential nature of any such information. Any Party who inadvertently fails to identify Documents as "Confidential," "Highly Confidential" or "Highly Confidential – Computer Source Code" may, within a reasonable time after discovering its failure, re-designate Documents by providing written notice of the error and substituted copies of the inadvertently produced Documents to the Recipient. Any Party receiving such inadvertently unmarked

Documents shall make reasonable efforts to retrieve Documents distributed to Persons not entitled to receive Documents with the corrected designation.

14. Nothing in this Order shall require production of information that a Party contends is protected from disclosure by the attorney-client privilege, the work product doctrine or other privilege, doctrine, right, or immunity. If information subject to a claim of attorney-client privilege, the work product doctrine or other privilege, doctrine, right, or immunity, is nevertheless inadvertently or unintentionally produced, such production shall in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any such privilege, doctrine, right or immunity. Any Party that inadvertently or unintentionally produces materials protected by the attorney-client privilege, the work product doctrine or other privilege, doctrine, right, or immunity, may obtain the return of those materials by notifying the Recipient in writing within a reasonable time after actually becoming aware of the inadvertent production and providing a privilege log within fifteen (15) days after notice for the inadvertently produced materials, unless both parties agree that it is not necessary. If such a request for return of information is made within a reasonable time, the Recipient shall gather and promptly return all copies of the privileged material to the Producer, except for any pages containing privileged markings by the Recipient, which pages shall instead be destroyed. Return of the information or material by the Recipient shall not constitute an admission or concession, or permit any inference, that the returned information or material is, in fact, properly subject to a claim of attorney-client privilege or work product immunity nor shall it foreclose any Party from moving the court for an order that such information or material has been improperly designated or should be producible for reasons other than a waiver caused by the inadvertent production. The Recipient shall certify in writing that all copies of the privileged materials have been returned and/or destroyed. This

Order constitutes a Federal Rule of Evidence 502(d) order, establishing that any inadvertently produced material subject to the attorney-client privilege or work product immunity is not a waiver as to Edge, Barclays, UBS, Wolverine, or any third party.

15. This Order does not, by itself, authorize the filing of any Document under seal. No Document may be filed under seal without prior leave of court. A Party wishing to file under seal a Document containing Confidential, Highly Confidential or Highly Confidential – Computer Source Code information must move the Court, consistent with Local Rule 26.2(b) and prior to the due date for the Document, for permission to file the Document under seal. If a Party obtains permission to file a Document under seal, it must also (unless excused by the Court) file a public-record version that excludes any Confidential, Highly Confidential or Highly Confidential – Computer Source Code information. If a Party wishes to file in the public record a Document that another Producer has designated as Confidential, Highly Confidential or Highly Confidential – Computer Source Code, the Party must advise the Producer of the Document no later than five (5) business days before the Document is due to be filed, so that the Producer may move the Court to require the Document to be filed under seal. Pursuant to Local Rule 5.8, any Document filed under seal must be accompanied by a cover sheet disclosing (i) the caption of the case, including the case number; (ii) the title “Restricted Document Pursuant to Local Rule 26.2;” (iii) a statement that the Document is filed as restricted in accordance with a court order and the date of the order; and (iv) the signature of the attorney of record filing the Document.

16. If a Party disputes a Producer’s designation of information as “Confidential,” “Highly Confidential” or “Highly Confidential – Computer Source Code,” the Party shall notify the Producer in writing of the basis for the dispute, identifying the specific Document(s) or thing(s) as to which the designation is disputed and proposing a new designation for such

materials. The Party and the Producer shall then meet and confer to attempt to resolve the dispute without involvement of the Court. If they cannot resolve the dispute, the proposed new designation shall be applied fourteen (14) days after notice of the dispute unless within that fourteen day period the Producer files a motion with the Court to maintain the Producer's designation. The Producer bears the burden of proving that the information is properly designated. The information shall remain subject to the Producer's designation until the Court rules on the dispute. A Party's failure to contest a designation of information is not an admission that the information was properly designated as such.

17. Within a reasonable amount of time of the termination of this action, including any appeals, each Party shall either destroy or return to the Producer all materials designated by the Producer as Confidential, Highly Confidential, or Highly Confidential – Computer Source Code, and all copies of such Documents, and shall destroy all extracts and/or data taken from such materials. Each Party's obligation to destroy or return materials stored in electronic format shall be limited to electronic data that is reasonably accessible to the Party, and shall not extend to offsite backup or archival media. Each Party shall provide a certification as to such return or destruction within the reasonable period of time. Attorneys shall be entitled to retain, however, copies of all pleadings, motions and trial briefs (including all supporting and opposing papers and exhibits), written discovery requests and responses (including exhibits), deposition transcripts and exhibits, expert reports and exhibits, trial transcripts, and exhibits offered or introduced into evidence at trial, correspondence, memoranda, notes and other work product materials. Additionally, any Party may retain Documents or information as needed to comply with regulatory requirements.

18. Any Party may apply to the Court for a modification of this Protective Order, and nothing in this Protective Order shall be construed to prevent a Party from seeking such further provisions enhancing or limiting confidentiality as may be appropriate.

19. Nothing in this Order shall be construed to prevent Attorneys from advising their clients with respect to this litigation based upon Confidential, Highly Confidential, or Highly Confidential – Computer Source Code information, provided the Attorneys do not disclose the Confidential, Highly Confidential, or Highly Confidential – Computer Source Code information itself, except as provided in this Order.

20. No action taken in accordance with this Protective Order shall be construed as a waiver of any claim or defense in the action or of any position as to discoverability or admissibility of evidence.

21. The obligations imposed by this Protective Order shall survive the conclusion of this case.

Date: September 27, 2011

  
Morton Denlow  
United States District Court Magistrate Judge

**EXHIBIT A**  
**WRITTEN ASSURANCE**

\_\_\_\_\_ declares that:

I reside at \_\_\_\_\_ in the city of \_\_\_\_\_, county \_\_\_\_\_, state of \_\_\_\_\_; I am currently employed by \_\_\_\_\_ located at \_\_\_\_\_ and my current job title is \_\_\_\_\_.

I have read and understand the terms of the Protective Order dated \_\_\_\_\_, filed in Civil Action No. 09-CV-1521, pending in the United States District Court for the Northern District of Illinois. I agree to comply with and be bound by the provisions of the Protective Order. I understand that any violation of the Protective Order may subject me to sanctions by the Court.

I shall not divulge any Documents, or copies of Documents, designated "Confidential," "Highly Confidential" or "Highly Confidential – Computer Source Code" obtained pursuant to the Protective Order, or the contents of such Documents, to any Person other than those specifically authorized by the Protective Order. I shall not copy or use such Documents except for the purposes of this action and pursuant to the terms of the Protective Order.

As soon as practical, but no later than 30 days after final termination of this action, I shall return to the attorney from whom I have received any Documents in my possession designated "Confidential," "Highly Confidential," or "Highly Confidential-Computer Source Code" and all copies, excerpts, summaries, notes, digests, abstracts, and indices relating to such Documents.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: \_\_\_\_\_, 20\_\_\_\_

\_\_\_\_\_